



John Doe
525 Junction Rd
Madison, WI 53717

March 31, 2022

IMPORTANT ACCOUNT SECURITY NOTICE

Dear John:

I am writing to let you know about a data security incident affecting your TDS Telecom email account. We are notifying you to explain the circumstances as we understand them, and to make you aware of the steps we have taken to respond and the resources we are making available to you.

What Happened?

Earlier this month, we discovered that an individual was impersonating TDS IT personnel to trick call center employees into granting remote access to their call center computer through multiple layers of security. TDS took immediate action to investigate the scope of the incident and determined that the fraudster was able to change the passwords and access a limited number of TDS customer email accounts on February 24, 2022 and March 16, 2022. TDS promptly initiated a password reset on the impacted accounts. We have also reported the incident to law enforcement.

What Information Was Involved?

Impacted information included information about your TDS Telecom email account, including recovery contacts (phone and/or email). While the fraudster was able to change your password and access a limited number of TDS email accounts, the prior password was not visible in the systems.

What We Are Doing

The safety of your personal information is of utmost importance to us. We investigated to understand the scope and impact of the incident and reported it federal law enforcement. In addition to changing passwords, we have also taken steps to further secure our systems and will continue to provide regular reminders to employees on how to identify social engineering attacks.

What You Can Do

We recommend that you pick unique and strong passwords, and not share them amongst other accounts. If you had used the same password for other accounts, we recommend you change that password as well to a different, unique and strong password. We also encourage you to remain vigilant and monitor your accounts for any suspicious activity and to report any suspected incidents of fraud to your financial




institution. We would also encourage you to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for your personal information or refer you to a website asking for personal information. Please refer to the enclosure entitled "Additional Ways to Protect Your Identity" for additional actions you should consider taking to protect yourself against fraud and identity theft.

For More Information

We take the security of your information very seriously and sincerely regret any inconvenience or concern. Should you have questions or concerns, please do not hesitate to contact the support team at 1 (888) 233-0001.

Sincerely,

DocuSigned by:


D0FD0AD5B41341A...

Karl Betz

VP-Information Technology & CISO



Additional Ways to Protect Your Identity: Important Identity Theft Information

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax

P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016-1000
1-888-909-8872
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/
personal/credit-report-
services/credit-freeze/](http://www.equifax.com/personal/credit-report-services/credit-freeze/)

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)



You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Complete addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts one (1)-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/fraud-victim-resource/place-fraud-alert

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, including your Attorney General and the FTC. You may also obtain additional information about security freezes and fraud alerts from the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov